2B Proof techniques

2B1 (Cartesian products) For each of the following equations, either prove it true, or prove it false by a concrete counterexample (an element of one side of the equation that is not an element of the other side).

(a) $(\mathbb{Z} \times \mathbb{R}) \cap (\mathbb{R} \times \mathbb{Z}) = \mathbb{Z} \times \mathbb{Z}$

(b) $(\mathbb{Z} \times \mathbb{R}) \cup (\mathbb{R} \times \mathbb{Z}) = \mathbb{R} \times \mathbb{R}$

Solution.

(a) True.

To show $(\mathbb{Z} \times \mathbb{R}) \cap (\mathbb{R} \times \mathbb{Z}) \subseteq \mathbb{Z} \times \mathbb{Z}$:

Let $(a, b) \in (\mathbb{Z} \times \mathbb{R}) \cap (\mathbb{R} \times \mathbb{Z})$. Then $(a, b) \in \mathbb{Z} \times \mathbb{R}$ and $(a, b) \in (\mathbb{R} \times \mathbb{Z})$. Hence both $a, b \in \mathbb{Z} \cap \mathbb{R} = \mathbb{Z}$. We conclude $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

To show $(\mathbb{Z} \times \mathbb{R}) \cap (\mathbb{R} \times \mathbb{Z}) \supseteq \mathbb{Z} \times \mathbb{Z}$:

Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Notice $\mathbb{Z} \times \mathbb{Z} \subset \mathbb{Z} \times \mathbb{R}$ and $\mathbb{Z} \times \mathbb{Z} \subset \mathbb{R} \times \mathbb{Z}$, because $\mathbb{Z} \subset \mathbb{R}$. Therefore $(a, b) \in \mathbb{Z} \times \mathbb{R}$ and $(a, b) \in \mathbb{R} \times \mathbb{Z}$. We conclude $(a, b) \in (\mathbb{Z} \times \mathbb{R}) \cap (\mathbb{R} \times \mathbb{Z})$.

(b) False. Counterexample: $(0.5, 0.5) \in \mathbb{R} \times \mathbb{R}$. But $(0.5, 0.5) \notin (\mathbb{Z} \times \mathbb{R})$ and $(0.5, 0.5) \notin (\mathbb{R} \times \mathbb{Z})$ because $0.5 \notin \mathbb{Z}$, so $(0.5, 0.5) \notin (\mathbb{Z} \times \mathbb{R}) \cup (\mathbb{R} \times \mathbb{Z})$.

2B2 (Parity) Prove that if $n \in \mathbb{Z}$, then $n^2 + 3n + 4$ is even. Hint: Direct proof by cases: case 1 for n even, and case 2 for n odd.

Solution. Case 1: Let $n \in \mathbb{Z}$ be arbitrary even integer. Then both n^2 and $3n$ are even, because any multiple of an even number is still even. Also, 4 is even. The sum of even numbers is even, therefore $n^2 + 3n + 4$ is even.

Case 2: Let $n \in \mathbb{Z}$ be arbitrary odd integer. Then both n^2 and $3n$ are odd because any odd multiple of an odd number is still odd. The sum of two odd numbers is even, therefore $n^2 + 3n$ is even. Finally 4 is even, and the sum of even numbers is even, therefore $n^2 + 3n + 4$ is even.

2B3 (Multi-way De Morgan) On the lectures we learned about De Morgan's law for two propositions. An obvious-looking generalization is the following claim (where $p_1, \ldots, p_n$ are arbitrary propositions):

$$\big(\neg(p_1 \vee \ldots \vee p_n)\big) \iff \big((\neg p_1) \wedge \ldots \wedge (\neg p_n)\big).$$

(a) Prove the claim for $n = 3$ directly by a truth table of 8 rows.

(b) For $n = 10$, how many rows would you need, if you wrote the full truth table explicitly? Can you characterize in just a few words how the table would look (on which rows would the results of the LHS and the RHS be "true", and on which rows would they be "false")?

(c) Prove the claim for all integers $n \geq 2$ by induction. (Hint: A conjunction of n propositions can be decomposed into a two-way conjunction of one proposition and the conjunction of the remaining $n - 1$.)

Solution.

(a) For the sake of space, define the shorthands $Q_1 = \big(\neg(p_1 \vee \ldots \vee p_n)\big)$ and $Q_2 = \big((\neg p_1) \wedge \ldots \wedge (\neg p_n)\big)$. The truth table is as follows:

p_1	p_2	p_3	$p_1 \vee p_2 \vee p_3$	Q_1	$\neg p_1$	$\neg p_2$	$\neg p_3$	Q_2	$Q_1 \Leftrightarrow Q_2$
0	0	0	0	1	1	1	1	1	1
0	0	1	1	0	1	1	0	0	1
0	1	0	1	0	1	0	1	0	1
0	1	1	1	0	1	0	0	0	1
1	0	0	1	0	0	1	1	0	1
1	0	1	1	0	0	1	0	0	1
1	1	0	1	0	0	0	1	0	1
1	1	1	1	0	0	0	0	0	1

In particular we observe that the truth values of Q_1 and Q_2 are identical, therefore $Q_1 \Leftrightarrow Q_2$ is always true.

(b) For $n = 10$ the truth table would consist of $2^{10} = 1024$ rows. Both the LHS and RHS propositions would be true only when $p_1, \ldots, p_{10}$ are all false.

(c) For the base case, we note that $P(2)$ has been already proven by a truth table.

For the induction step, we will prove that if $n \geq 2$ and $P(n)$ is true, then also $P(n + 1)$ is true. The method is to break the $(n + 1)$-way disjunctions and conjunctions into smaller ones, to which we can apply the smaller cases of De Morgan.[1]

[1] We assume that e.g. $p_1 \wedge \ldots p_n \wedge p_{n+1}$ is *defined* by putting parentheses around the first n propositions, that is, $(p_1 \wedge \ldots p_n) \wedge p_{n+1}$. Similarly for the disjunction. If we had proven the associativity of big conjunctions and disjunctions, we could also put parentheses anywhere, but that is not needed here.

$$\begin{aligned} & \neg\left(p_1 \vee \ldots \vee p_n \vee p_{n+1}\right) & \\ \iff & \neg\Big(\left(p_1 \vee \ldots \vee p_n\right) \;\vee\; p_{n+1}\Big) & \text{(Added parentheses)} \\ \iff & \Big(\neg\left(p_1 \vee \ldots \vee p_n\right)\Big) \;\wedge\; \left(\neg p_{n+1}\right) & \text{(By } P(2)\text{)} \\ \iff & \Big(\left(\neg p_1\right) \wedge \ldots \wedge \left(\neg p_n\right)\Big) \;\wedge\; \left(\neg p_{n+1}\right) & \text{(By } P(n)\text{)} \\ \iff & \left(\neg p_1\right) \wedge \ldots \wedge \left(\neg p_n\right) \;\wedge\; \left(\neg p_{n+1}\right). & \text{(Removed parentheses)} \end{aligned}$$

By induction we have proven $P(n)$ for all integers $n \geq 2$.

Note the method of stringing together *several* equivalent propositions. This is *understood* as a conjunction: that the first is equivalent to the second, *and* the second is equivalent to the third, and so on. This proves that the first is equivalent to the last, just like a long equation like $a = b = c = d$ proves $a = d$. This method is very compact but should be used with care, because every step really has to be an *equivalence*, not only an implication. A string of implications to the right would only prove an implication, not equivalence. (Likewise, in arithmetic, $a = b \leq c = d$ does not prove $a = d$, but it proves $a \leq d$.)

Thinking of the reader, a long string of symbolic math can be difficult to follow. You can help the reader by hinting, on each line, why the step is equivalent with the previous one.

Alternative proof. We argue that for each of the LHS and RHS proposition, it is true if and only if all $p_1, \ldots, p_n$ are false. The claim then follows.

For the LHS proposition: Let $n \in \mathbb{N}$ be arbitrary. Suppose $p_1, \ldots, p_n$ are all false, then $p_1 \vee \ldots \vee p_n$ is false, therefore $\big(\neg(p_1 \vee \ldots \vee p_n)\big)$ is true. On the other hand, suppose not all $p_1, \ldots, p_n$ are false, that is, at least one of them is true. Then $p_1 \vee \ldots \vee p_n$ is true, and hence $\big(\neg(p_1 \vee \ldots \vee p_n)\big)$ is false. We conclude $\big(\neg(p_1 \vee \ldots \vee p_n)\big)$ is true if and only if $p_1, \ldots, p_n$ are all false.

For the RHS proposition: We argue by induction. Define the statement $P(n)$: $\big((\neg p_1) \wedge \ldots \wedge (\neg p_n)\big)$ is true if and only if $p_1, \ldots, p_n$ are false.

Consider $P(1)$. If p_1 is false, then $(\neg p_1)$ is true. On the other hand if p_1 is true, then $(\neg p_1)$ is false. Therefore $P(1)$ is true.

Assume that $P(n)$ is true for some $n \in \mathbb{N} \setminus \{0\}$. Consider $P(n+1)$.

Suppose all $p_1, \ldots, p_{n+1}$ are false. Then $(\neg p_{n+1})$ is true, and by assumption $\big((\neg p_1) \wedge \ldots \wedge (\neg p_n)\big)$ is also true. Therefore $\big((\neg p_1) \wedge \ldots \wedge (\neg p_{n+1})\big) = \big((\neg p_1) \wedge \ldots \wedge (\neg p_n)\big) \wedge (\neg p_{n+1})$ is true.

On the other hand, suppose not all $p_1, \ldots, p_{n+1}$ are false, that is, at least one of them is true. Consider two cases below:

Case 1: At least one of $p_1, \ldots, p_n$ is true. Then by assumption $\big((\neg p_1) \wedge \ldots \wedge (\neg p_n)\big)$ is false. Therefore $\big((\neg p_1) \wedge \ldots \wedge (\neg p_{n+1})\big) = \big((\neg p_1) \wedge \ldots \wedge (\neg p_n)\big) \wedge (\neg p_{n+1})$ is false, regardless of what p_{n+1} is.

Case 2: All of $p_1, \ldots, p_n$ are false. Then p_{n+1} must be true, and $(\neg p_{n+1})$ is false. Therefore $\big((\neg p_1) \wedge \ldots \wedge (\neg p_{n+1})\big) = \big((\neg p_1) \wedge \ldots \wedge (\neg p_n)\big) \wedge (\neg p_{n+1})$ is false, regardless of what $\big((\neg p_1) \wedge \ldots \wedge (\neg p_n)\big)$ is.

Putting together, we conclude that $P(n+1)$ is true. By induction, $P(n)$ is true for all $n \in \mathbb{N} \setminus \{0\}$.

2B4 (Sums of powers)

(a) Prove by induction that $\sum_{j=0}^{n} 2^j = 2^{n+1} - 1$ for all integers $n \geq 0$.

(b) Prove by induction that $\sum_{j=0}^{n} 3^j = (3^{n+1} - 1)/2$ for all integers $n \geq 0$.

(c) Prove by induction that $\sum_{j=0}^{n} 10^j = (10^{n+1} - 1)/9$ for all integers $n \geq 0$. Calculate a few first values of the LHS and RHS. Does the result look obvious?

Solution.

(a) Define the statement $P(n)$: $\sum_{j=0}^{n} 2^j = 2^{n+1} - 1$.

For $P(0)$, we have

$$\text{LHS} = 2^0 = 1 = 2 - 1 = 2^{0+1} - 1 = \text{RHS}.$$

Therefore $P(0)$ is true.

Assume $P(n)$ is true for some $n \in \mathbb{N}$. For $P(n+1)$, we have

$$\text{LHS} = \sum_{j=0}^{n+1} 2^j = \sum_{j=0}^{n} 2^j + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2^{n+2} - 1 = \text{RHS},$$

where the third equality follows from the assumption. Therefore $P(n+1)$ is true. By induction $P(n)$ is true for all $n \in \mathbb{N}$.

(b) Define the statement $P(n)$: $\sum_{j=0}^{n} 3^j = (3^{n+1} - 1)/2$.

For $P(0)$, we have

$$\text{LHS} = 3^0 = 1 = (3^{0+1} - 1)/2 = \text{RHS}.$$

Therefore $P(0)$ is true.

Assume $P(n)$ is true for some $n \in \mathbb{N}$. For $P(n+1)$, we have

$$\begin{aligned}\text{LHS} = \sum_{j=0}^{n+1} 3^j &= \sum_{j=0}^{n} 3^j + 3^{n+1} \\ &= (3^{n+1} - 1)/2 + 3^{n+1} \\ &= (3^{n+1} - 1 + 3^{n+1} \cdot 2)/2 = (3^{n+2} - 1)/2 = \text{RHS},\end{aligned}$$

where the third equality follows from the assumption. Therefore $P(n+1)$ is true. By induction $P(n)$ is true for all $n \in \mathbb{N}$.

(c) Define the statement $P(n)$: $\sum_{j=0}^{n} 10^j = (10^{n+1}-1)/9$.

For $P(0)$, we have

$$\text{LHS} = 10^0 = 1 = (10^{0+1}-1)/9 = \text{RHS}.$$

Therefore $P(0)$ is true.

Assume $P(n)$ is true for some $n \in \mathbb{N}$. For $P(n+1)$, we have

$$\begin{aligned}\text{LHS} = \sum_{j=0}^{n+1} 10^j &= \sum_{j=0}^{n} 10^j + 10^{n+1} \\ &= (10^{n+1}-1)/9 + 10^{n+1} \\ &= (10^{n+1}-1+10^{n+1}\cdot 9)/9 = (10^{n+2}-1)/9 = \text{RHS},\end{aligned}$$

where the third equality follows from the assumption. Therefore $P(n+1)$ is true. By induction $P(n)$ is true for all $n \in \mathbb{N}$.

Some concrete examples: For $n = 1$, we have $11 = (100-1)/9$; For $n = 2$, we have $111 = (1000-1)/9$, and so on.

2B5 (Faulty induction) Consider all one-colored socks in the world. (For brevity we will just call them "socks". We do not consider socks that contain multiple colors.) We assume here that color is a well-defined property: the colors of any two socks are either same or different. Here is a purported proof that *all socks in the world have the same color.*

"Proof." For every integer $n \geq 1$, let $P(n)$ be the claim "Every collection of n socks is unicolored" (i.e. the socks in the collection have the same color). We prove by induction that $P(n)$ is true for all n. In particular, $P(n)$ is true when n is the number of all socks in the world. Find the error in this proof.

- Base case: Clearly $P(1)$ is true, because in any one-sock collection there is only one color.

- Induction step: Suppose that for some n, $P(n)$ is true. We will prove that $P(n+1)$ is then also true. Consider any collection of $n+1$ socks, and name its socks $s_1, s_2, \ldots, s_{n+1}$. By the induction hypothesis, the first n socks $(s_1, \ldots, s_n)$ all have the same color. Also by the induction hypothesis, the last n socks $(s_2, \ldots, s_{n+1})$ have the same color. Because s_1 has the same color as s_2, and all the remaining socks also have the same color as s_2, clearly all $n+1$ socks have the same color.

- By the induction principle, $P(n)$ is true for all n. The proof is complete.

Solution. The argument on $P(n+1)$ is not sound. There it is implicitly assumed that for any $n \in \mathbb{N}$, for the set $\{s_1, \ldots, s_{n+1}\}$ of $n+1$ socks, there exist two different non-empty subsets S_1 and S_2, both of size at most n, such that $S_1 \cap S_2 \neq \emptyset$ and $S_1 \cup S_2 = \{s_1, \ldots, s_{n+1}\}$. E.g. $S_1 = \{s_1, \ldots, s_n\}$ and $S_2 = \{s_2 \ldots, s_{n+1}\}$ with the intersection $\{s_2, \ldots, s_n\}$ as stated. But this assumption is false. In particular, when $n = 1$, for the set $\{s_1, s_2\}$ of socks, the only non-empty subsets of size 1 are $\{s_1\}$ and $\{s_2\}$, which have an empty intersection.

2B6 (Fibonacci parity) The Fibonacci numbers are the sequence $f_0, f_1, f_2, \ldots$ where $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ when $n \geq 2$.

(a) Calculate the first ten Fibonacci numbers $f_0, \ldots, f_9$ and circle those that are even.

(b) Study the indices n of your circled numbers, and guess a very simple rule that allows you, by looking at the index n to decide whether f_n is even or odd (without having to calculate f_n).

(c) Prove your rule for all $n \in \mathbb{N}$ by induction.

Solution.

(a) $f_0 = 0$, $f_1 = 1$, $f_2 = 1$, $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, $f_6 = 8$, $f_7 = 13$, $f_8 = 21$, $f_9 = 34$. The ones that are even are f_0, f_3, f_6, f_9.

(b) A natural guess is that f_n is even if n is a multiple of 3, and otherwise odd.

(c) Statement $P(n)$: f_n is even if n is a multiple of 3, and f_n is odd otherwise.

For $P(0)$, we have $f_0 = 0$ by definition, which is even, and 0 is a multiple of 3. For $P(1)$, we have $f_1 = 1$ by definition, which is odd, and 1 is not a multiple of 3. Therefore the statement is true for $P(0)$ and $P(1)$.

Suppose $P(n-1)$ and $P(n)$ are true for some $n \in \mathbb{N} \setminus \{0\}$. Consider two cases for $P(n+1)$.

Case 1: $n+1$ is a multiple of 3. Then both $n-1$ and n are not multiple of 3, and by assumption both f_{n-1} and f_n are odd. The sum of two odd numbers is even, therefore $f_{n+1} = f_{n-1} + f_n$ is even.

Case 2: $n+1$ is not a multiple of 3. Then one (and only one) of $n-1$ and n is a multiple of 3, and by assumption one of f_{n-1} and f_n is odd, another one is even. The sum of one odd and one even number is odd, therefore $f_{n+1} = f_{n-1} + f_n$ is odd.

Putting the two cases together, we have that $P(n+1)$ is true. By induction, $P(n)$ is true for all $n \in \mathbb{N}$.

Again the “challenge” problem is worth an extra point. That is, by doing any six problems (whether it includes the challenge problem or not) you gain six points, which is considered 100% of this set. By doing all seven you gain seven points, which is considered $7/6 = 116\frac{2}{3}\%$.

2B7 (** CHALLENGE: Golomb rulers) A **Golomb ruler** is a set $A \subseteq \mathbb{Z}$, where the smallest element is zero, and each pair of elements has a different distance (between its two elements).[2] Distance means arithmetic difference. For example, $\{0, 1, 2\}$ is *not* a Golomb ruler, because between 0 and 1 there is the same distance as between 1 and 2. But $\{0, 1, 5\}$ *is* a Golomb ruler, because all its pairs have different distances: $1-0 = 1$, $5-1 = 4$ and $5-0 = 5$. (We do not consider distances of elements to themselves — they would of course all be zero — and we only consider the positive distances $b - a$ where $b > a$.) The *length* of a ruler is the distance between its smallest and largest element. Golomb rulers have real-world applications in error-correcting codes, X-ray crystallography, radio frequency selection and radio antenna placement. One common problem is to find the *shortest* Golomb ruler of a given cardinality. The elements are called "marks" in analogy to actual rulers.

(a) Find a Golomb ruler with three marks and length 3.

(b) Prove that there is no Golomb ruler with three marks and length smaller than 3.

(c) Find a shortest possible Golomb ruler with four marks. Prove that there is no shorter one. (Hint: It is probably a good idea to break into cases. There are many different ways of doing that.)

Solution.

(a) One example is $\{0, 1, 3\}$. Its length is $3 - 0 = 3$. It is straightforward to verify that the pair-wise distances are $1, 2, 3$.

(b) Suppose (towards contradiction) that there exists such a Golomb ruler. Let it be $\{a, b, c\}$ where $a = 0$ and $b, c \in \mathbb{Z}$. Without loss of generality assume $b < c$. Since the length is smaller than 3, we have either $c = 1$ or $c = 2$. But $c = 1$ is not possible, since this contradicts with the existence of b where $0 < b < 1$. Therefore $c = 2$, and the only possibility of b is 1. But then the distance between a, b and that between b, c are both 1, a contradiction to the definition of a Golomb ruler. We conclude that there does not exist a Golomb ruler with 3 marks and length smaller than 3.

(c) One example is $\{0, 1, 4, 6\}$, of length 6. Below we show that there does not exist a Golomb ruler with 4 marks and of length smaller than 6.

Suppose (towards contradiction) that there exists such a Golomb ruler. Let it be $\{a, b, c, d\}$ for some $a, b, c, d \in \mathbb{Z}$. Without loss of generality assume $a = 0$ and $a < b < c < d$. Since the length is smaller than 6, we have d equals either $1, 2, 3, 4$ or 5. That d equals 1 or 2 is not possible, since this contradicts with the existence of two distinct integers b, c where $0 < b < c < d$. Therefore d equals $3, 4$ or 5.

[2] The usual definition does not require the smallest element to be zero, but here we do so for simplicity.

Suppose $d = 3$. Then the only possibility of b, c is $b = 1$ and $c = 2$. But then the distance between a, b and that between b, c are both 1, a contradiction to the definition of a Golomb ruler. So $d = 3$ is not possible.

Next suppose $d = 4$. Consider the possibilities of b, c here. With the same argument as above, we know that $b = 1$ and $c = 2$ is not possible. There are two cases left. The first is $b = 2$ and $c = 3$, but the distance between b, c and that between c, d are both 1, a contradiction to the definition of a Golomb ruler. The second is $b = 1$ and $c = 3$, but then the distance between a, b and that between c, d are both 1, a contradiction.

The only remaining case is $d = 5$. With the same argument as above, we know that $b = 1$ and $c = 2$ is not possible. The remaining possibilities of (b, c) are $(1, 3), (1, 4), (2, 3), (2, 4)$ and $(3, 4)$. We check all cases. If $(b, c) = (1, 3)$ then $c - b = d - c = 2$, a contradiction. If $(b, c) = (1, 4)$ then $b - a = d - c = 1$, a contradiction. If $(b, c) = (2, 3)$ then $b - a = d - c = 2$, a contradiction. If $(b, c) = (2, 4)$ then $b - a = c - b = 2$, a contradiction. If $(b, c) = (3, 4)$ then $c - b = d - c = 1$, a contradiction.

In all cases we have a contradiction. Therefore we conclude that there does not exist a Golomb ruler with 4 marks and length smaller than 6.

If you want to learn more about Golomb rulers, see for example the Wikipedia page Golomb ruler. Today the minimum-length Golomb rulers are known up to 28 marks. The 28-mark ruler was determined through a massive distributed computation using the spare time of thousands of computers, beginning in 2014 and finishing in 2022, see distributed.net: Completion of OGR-28 project.